Novembre 2014

La CNIL : mode d'emploi

Au quotidien, les collectivités ont de plus en plus recours aux outils informatiques pour gérer les services dont elles ont la compétence. Simultanément les échanges entre administrations et avec les usagers se dématérialisent. L'ensemble de ces outils informatiques et services d'e-administration contiennent de nombreuses informations à caractère personnel qui concernent des personnes physiques. La loi informatique et libertés du 6 janvier 1978 modifiée fixe un cadre à la collecte, au traitement et à la conservation de ces informations afin de protéger les droits fondamentaux dont la vie privée de chacun d'entre nous.

CNIL-Commission nationale de l'informatique et des libertés
La CNIL est une autorité administrative indépendante chargée de veiller au respect des dispositions de la loi du 6 janvier 1978 : à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Qu'est-ce qu'une information à caractère personnel ?
Une information permettant d'identifier directement ou indirectement (par recoupement d'informations) une personne physique.
Les informations peuvent être directement nominatives, comme le nom, le prénom, une photographie ou indirectement nominatives, comme un n° d'immatriculation, une adresse IP, un numéro de dossier, un RIB.
Certaines informations bénéficient d'une protection supplémentaire :
- Données sensibles : ce sont les données qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, l'état de santé ou la vie sexuelle
- Données relatives aux infractions, condamnations et mesures de sûreté
- NIR : numéro de sécurité sociale

La société SPL X-demat propose à ses adhérents des services d'e-administration. Pour autant, en tant que maire ou président vous êtes responsable de la collecte, du traitement et de la conservation des informations enregistrées dans les applications informatiques fournies par la société SPL X-demat et plus généralement de l'utilisation qui est faite des données collectées.

Du point de vue de la réglementation informatique et libertés, la collectivité est le responsable de traitement et la société SPL X-demat prestataire de service ou sous-traitant pour le compte du responsable de traitement. C'est à chaque collectivité de veiller au respect des cinq principes cadres fixés par la loi informatique et libertés.

Cinq principes doivent être respectés concurremment :

- **Principe de finalité** : les informations ne peuvent être recueillies et traitées que pour un usage déterminé et légitime qui doit correspondre aux missions de la collectivité
- **Principe de proportionnalité** : seules doivent être traitées les informations pertinentes et nécessaires pour la gestion desdites missions de la collectivité
- **Principe d'une durée limitée de conservation des informations** : les informations ne peuvent pas être conservées de manière illimitée ; la durée de conservation doit être définie à l'avance et, dans tous les cas, adaptée à la finalité du traitement. Cette durée peut être très variable en fonction des traitements, de quelques mois à plusieurs dizaines d'années.

- **Principe de sécurité et de confidentialité des informations** : le maire ou le président est responsable de la sécurité des informations ; il doit garantir leur confidentialité et s'assurer qu'elles ne sont pas communiquées à des personnes non autorisées.
- **Principe du respect des droits des personnes** : lors du recueil des informations, les usagers doivent être informés de la finalité du traitement, du caractère obligatoire ou facultatif des réponses, des destinataires des informations et de leurs droits -droit d'accès, de rectification, de suppression, voire dans certains cas droit de s'opposer à ce que des informations les concernant soient enregistrées.

Les bonnes pratiques

- Déclarer le traitement auprès de la CNIL
- Informer les usagers
- Mettre en œuvre des mesures de sécurité adéquates

Qu'est-ce qu'un traitement ?

Un « traitement de données à caractère personnel » est une notion très large. Il s'agit de toute opération portant sur des données à caractère personnel, quel que soit le procédé technique utilisé, notamment la collecte, l'enregistrement, la conservation, la modification, l'extraction, la consultation, la communication, le transfert.

Comment déclarer ?

La déclaration doit être préalable à la mise en œuvre du traitement.

Il existe plusieurs régimes de formalité, selon la finalité du traitement et/ou le degré de sensibilité des données collectées :

- Dispense de formalité
- Déclaration simple
- Demande d'avis
- Demande d'autorisation

Applications fournies par la SPL Xdémat : comment se mettre en conformité ?

Nom de l'application	Finalités	Observations
Dispenses de déclaration		
Xelec	Gestion du fichier électoral	Dispense n°12 (gestion du fichier électoral)
Xactes	Télétransmission des actes soumis au contrôle de légalité	Dispense n° 5 (traitements mis en œuvre par les collectivités et les services de l'Etat dans le cadre de la dématérialisation du contrôle de légalité)
Xmarchés	Dématérialisation des marchés publics	Dispense n° 3 (traitements mis en œuvre par les organismes publics dans le cadre de la dématérialisation des marchés publics)
Xfluco	Télétransmission des flux comptables	Dispense : délibération CNIL 80-34 du 21 octobre 1980 (traitement automatisé de la comptabilité générale) Dispense n°4 (gestion des fichiers fournisseurs)
Xfluco	Outil de recherche des flux télétransmis (référence comptable et nom du tiers)	Dispense : délibération CNIL 80-34 du 21 octobre 1980 (traitement automatisé de la comptabilité générale) Dispense n°4 (gestion des fichiers fournisseurs)
Déclaration de conformité		

Xmanager	**Administration des comptes utilisateurs** pour l'accès aux services d'e-administration fournis par la SPL Xdemat	Déclaration de conformité à la NS n°46
Xsip	**Vérification des éléments de facturation et suivi du paiement des titres de recettes et factures en régie**	Déclaration de conformité à la NS n° 27 (communes >2000 habitants) Déclaration de conformité à la NS n° 32 (communes <2000 habitants)
Déclaration simple		
Xconvoc	**Gestion des assemblées** : convocations, ordres du jour, suivi des présents, des mandats et des votes	
Xactes	**Outil d'indexation et de recherche des actes et délibérations produits par la collectivité**	
Xrecensement citoyen obligatoire	**Gestion du recensement militaire des jeunes de la commune** : impression des documents et listes associés, gestion dématérialisée des flux vers le bureau du Service National via le protocole PECOTO, archivage	
Pas de formalité spécifique		
Xs@re	Envoi en recommandé électronique	Ne correspond pas, en tant que telle, à une finalité au sens de la loi « Informatique et Libertés » ; par ailleurs, les documents concernés se rattachent à des traitements qui ont fait (ou doivent faire) l'objet des formalités préalables requises
Xsacha	Archivage électronique	
Xparaph	Parapheur électronique	

La collectivité peut désigner un correspondant Informatique et Libertés (CIL). Cette désignation exonère notamment de déclaration la plupart des traitements. C'est le CIL qui tient à jour la liste des traitements exonérés. Le CIL contribue par ailleurs à diffuser une culture « informatique et libertés ».

Communes de moins de 2000 habitants : régime de déclaration simplifié
Les communes de moins de 2000 habitants disposent d'un régime de déclaration simplifié pour l'ensemble des traitements concernant les relations avec la population (état civil, listes électorales, cantine, crèche, bibliothèque, etc.) : il s'agit de la norme simplifié n° 32.

Comment informer ?

Les informations suivantes doivent être portées à la connaissance des personnes concernées par le traitement (usagers ou agents) :
- Identité du responsable du traitement
- Finalité du traitement
- Destinataires des informations collectées
- Droits des personnes concernées
- Services auprès desquels ces droits peuvent être exercés

L'information doit être délivrée au moment du recueil des données à caractère personnel :
Par questionnaire : l'information doit figurer sur le questionnaire ainsi que le caractère obligatoire ou facultatif des réponses

Au guichet de la collectivité : l'information peut être diffusée au moyen d'affiches apposées dans les services ou par remise d'une plaquette d'information. Le site internet de la collectivité est également le moyen d'informer les personnes de leurs droits.
Lorsque les informations ne sont pas collectées directement auprès de l'intéressé, l'information est fournie lors du premier contact avec lui (par courrier, par exemple).

Exemple de mention CNIL à faire figurer sur les formulaires
Veuillez indiquer l'identité du responsable du traitement)
« Les informations recueillies font l'objet d'un traitement informatique destiné à … *(Veuillez préciser la finalité)*. Les destinataires des données sont :……………………… *(précisez)*.
Conformément à la loi « informatique et libertés » du 6 janvier 1978 modifiée en 2004, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent, que vous pouvez exercer en vous adressant à …………………………………… *(Veuillez préciser le service et l'adresse)*.
Vous pouvez également, pour des motifs légitimes, vous opposer au traitement des données vous concernant.

Quelles mesures de sécurité ?

Il s'agit notamment de mesures techniques mises en œuvre par la société SPL X-demat mais pas seulement : le principal risque en matière informatique est l'erreur humaine….les utilisateurs doivent être sensibilisés et sensibles au fait qu'ils manipulent des données à caractère personnel, qu'il s'agit pour l'essentiel de données confidentielles et qu'elles ne doivent être communiquées qu'aux seules personnes autorisées.

Pour en savoir plus

Le site Internet de la CNIL fournit de nombreux renseignements et guides pratiques.
Un service d'accueil téléphonique est également assuré par la CNIL